WHAT IS CLAIMED IS:

1. A cryptographic system in a computer system, said cryptographic system comprising:

at least one server;

a database, said database constructed and arranged to contain sensitive information, said database responsive to signals from one of said at least one server;

a key repository process on one of said at least one server, said key repository having two master keys, said two master keys constructed and arranged to manage information in said database, said key repository further constructed and arranged to authorize access to said sensitive information in said database;

at least one operator, said at least one operator having access to a first of said master keys; and

at least two owners, each of said owners having a portion of a second of said master keys;

wherein said at least operator and at least one of said owners are required to start said key repository process.

2. A cryptographic system as in claim 1 wherein said operator is enabled to assert that said computer system is genuine.

3. A cryptographic system as in claim 2 wherein if said operator asserts that said computer system is genuine, then said computer system is enabled to unlock and expose a set of cryptographic credentials that can be used by said key repository.

4. A cryptographic system as in claim 1 wherein said first master key is an integrity key.

5. A cryptographic system as in claim 1 wherein said first master key is a protection key.

6. A cryptographic system as in claim 1 wherein said second master key is an integrity key.

7. A cryptographic system as in claim 1 wherein said second master key is a protection key.

8. A cryptographic system as in claim 1 wherein said second master key is assembled from a set of secrets that are split among a plurality of owners.

9. A cryptographic system as in claim 8 wherein said second master key is assembled from a set of secrets that are split among a plurality of owners according to the Bloom-Shamir methodology.

10. A cryptographic system in a computer system, said cryptographic system comprising:

at least one server;

a database, said database constructed and arranged to contain sensitive information, said sensitive information including authentication information for at least one operator and at least two owners, said database responsive to signals from one of said at least one server;

a key repository process on one of said at least one server, said key repository having two master keys, said two master keys constructed and arranged to manage said sensitive information in said database, said key repository further constructed and arranged to retrieve said authentication information from said database;

wherein one of said operators authenticates himself, and at least one owner authenticates himself in order for said key repository process to restart.

11. A cryptographic system as in claim 10, wherein said one or more of said master keys is exposed upon restart of said key repository.

12. A cryptographic system as in claim 10, wherein at least one of said owners must approve all changes to said database that affect the security of said computer system.

13. A cryptographic system as in claim 10, wherein at least one of said owners must approve the addition of an owner.

14. A cryptographic system as in claim 10, wherein at least one of said owners must approve the addition of an operator.

15. A cryptographic system as in claim 10, wherein at least one of said owners must approve the addition of an owner and an operator.

16. A cryptographic system as in claim 10, wherein at least one of said owners must approve the removal of an owner.

17. A cryptographic system as in claim 10, wherein at least one of said owners must approve the removal of an operator.

18. A cryptographic system as in claim 10, wherein at least one of said owners must approve the removal of an owner and an operator.

19. A cryptographic system as in claim 10, wherein at least two of said owners must approve the addition of an owner.

20. A cryptographic system as in claim 10, wherein at least two of said owners must approve the addition of an operator.

21. A cryptographic system as in claim 10, wherein at least two of said owners must approve the addition of an owner and an operator.

22. A cryptographic system as in claim 10, wherein at least two of said owners must approve the removal of an owner.

23. A cryptographic system as in claim 10, wherein at least two of said owners must approve the removal of an operator.

24. A cryptographic system as in claim 10, wherein at least two of said owners must approve the removal of an owner and an operator.

25. A cryptographic system as in claim 10, wherein at least one of said owners must approve a change in the minimum number of owners required to restart said key repository.

26. A cryptographic system as in claim 10, wherein at least two of said owners must approve a change in the minimum number of owners required to restart said key repository.

27. A cryptographic system as in claim 10, wherein at least one of said owners must approve a change in the minimum number of owners required to restart said key repository.

28. A cryptographic system as in claim 10, wherein at least two of said owners must approve a change in the minimum number of owners required to restart said key repository.

29. A cryptographic system as in claim 10, wherein at least one of said owners must approve a change in the approval count.

30. A cryptographic system as in claim 10, wherein at least two of said owners must approve a change in the approval count.

31. A cryptographic system as in claim 10 wherein if said operator asserts that said computer system is genuine, then said computer system is enabled to unlock and expose a set of cryptographic credentials that can be used by said key repository.

32. A cryptographic system as in claim 10 wherein said first master key is an integrity key.

33. A cryptographic system as in claim 10 wherein said first master key is a protection key.

34. A cryptographic system as in claim 10 wherein said second master key is an integrity key.

35. A cryptographic system as in claim 10 wherein said second master key is a protection key.

36. A cryptographic system as in claim 10 wherein said second master key is assembled from a set of secrets that are split among a plurality of owners.

37. A cryptographic system as in claim 36 wherein said second master key is assembled from a set of secrets that are split among a plurality of owners according to the Bloom-Shamir methodology.

38. A cryptographic system in a computer system, said cryptographic system comprising:

at least one server;

a database, said database constructed and arranged to contain sensitive information, said database responsive to signals from one of said at least one server;

a key repository process on one of said at least one server, said key repository having at least one master key, said at least one master key being constructed and arranged to manage information in said database, said key repository further constructed and arranged to authorize access to said sensitive information in said database;

at least one operator, said at least one operator having access to said at least one master key; and

at least two owners, each of said owners having a portion of a at least one master key;

wherein said at least operator and at least one of said owners are required to start said key repository process.

39. A cryptographic system as in claim 38 wherein said operator is enabled to assert that said computer system is genuine.

40. A cryptographic system as in claim 39 wherein if said operator asserts that said computer system is genuine, then said computer system is enabled to unlock and expose a set of cryptographic credentials that can be used by said key repository.

41. A cryptographic system as in claim 38 wherein said at least one master key is an integrity key.

42. A cryptographic system as in claim 38 wherein said at least one master key is a protection key.

43. A cryptographic system as in claim 38 wherein said at least one master key is assembled from a set of secrets that are split among a plurality of owners.

44. A cryptographic system as in claim 43 wherein said at least one master key is assembled from a set of secrets that are split among a plurality of owners according to the Bloom-Shamir methodology.

Express Mail Label No. EV 035 974 805 US